Local Government Association (LGA) Briefing, Investigatory Powers Bill, House of Commons, Second Reading

15 March 2016

Briefing

Key messages

- The LGA supports the intention of the Investigatory Powers Bill which seeks to retain councils' access to communications data as defined in Clauses 53 and 64. We also support Clause 223 which introduces the new definitions of communications data with 'entities' and 'events' data replacing subscriber, service use and traffic data.

- Although they are not the main users of communications data, teams within councils, such as trading standards, use communications data to tackle a range of criminal activity and fraud. It is vital that the powers to access communications data identified in Clauses 53 and 64 keep pace with the technology through which an increasing amount of criminal activity is perpetrated, and councils continue to retain these powers.

- Councils will remain subject to more stringent oversight than any other body accessing communications data due to the requirement for them to seek judicial authorisation before accessing communications data. The LGA supports the safeguards identified in Clause 66 as an important means of ensuring public confidence. We are calling for the process of judicial authorisation to be more efficient so that it does not hinder appropriate use of communications data by councils.

Further Information

Current use of communications data

In the year to March 2015, there were 230,000 fraud offences reported to Action Fraud. Equivalent to four recorded offences per 1000 head of population, this is twice the rate of theft and four times the rate of robbery reported to the police.

Local authorities have an important role in protecting consumers and businesses from these and similar types of criminal activity. Often those involved, like rogue traders and loan sharks, prey on the most vulnerable in society.

Communications data is used by local authority trading standards teams to tackle scams and other activities that defraud businesses and consumers. This ranges from doorstep crime which targets vulnerable and elderly people to large scale cybercrime which is often conducted remotely.

Charities who work with victims who are most at risk from these types of scams have endorsed the importance of councils retaining the right to access communications data. For example Age UK states: 'We know that scams are a huge and under-reported problem – recent ONS statistics estimated over 5 million incidents of fraud in a year. We also know that fraudsters target older people, exploiting those who live with dementia or are lonely. Some people are so lonely

Rachel Phelps, Public Affairs and Campaigns Adviser
Email: Rachel.Phelps@local.gov.uk
Tel 020 7664 3119
Information centre 020 7664 3131 www.local.gov.uk

that they welcome the human contact in the scam letters they receive, or can be persuaded to trust people who turn up at the door offering to fix a problem for them, not realising them to be fraudulent'.

'In this context, trading standards officers have an essential role to play in protecting older people. If we want to tackle this growing threat to people's wealth and health, we need to ensure councils have all the tools they need. Failure to do this means leaving older people open to continual attack and, ultimately, more pressure on the state, with victims who lose everything potentially needing health and care services and welfare benefits'.

Corporate fraud teams in councils also use communications data to prevent fraud against local taxpayers, for example, tenancy fraud, right to buy fraud, social care fraud, insurance fraud and procurement fraud.

The importance of councils being able to access communications data has also been endorsed outside of local government. The Independent Reviewer of Terrorism Legislation (IRTL) concluded in a report last year that communications data is "properly and productively used… in combating a wide range of other crimes, most of them more prevalent than terrorism and some of them just as capable of destroying lives."

Although it is extremely important that councils maintain their right to access communications data in order to undertake their work, it should be noted that councils are not the primary users of communications data. The most recent Report of the Interception of Communications Commissioner noted that councils were responsible for just 0.4 per cent of all notices and authorisations to access communications data in 2014. [1]

The LGA and support the powers set out in the Investigatory Powers Bill, which maintain councils ability to access communications data under the new definitions of 'entity' and 'events' data.

Definitions of 'entity' and 'events' data

Entity data means any data which is about 'an entity, an association between a telecommunications service and an entity, or an association between any part of a telecommunication system and an entity.'

Events data means any data which 'identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time'. In amending the definitions of communications data, the LGA has called for the Government to ensure that there is full clarity about the types of data falling within each new category so that there is a transparent and accountable process.

Safeguards and offences

There is a need for a range of safeguards to provide public reassurance that councils use communications data appropriately. Only 19 out of 6,000 (0.3 per cent) council applications to access communications data were refused by magistrates between 2012 to 2015. This confirms that the powers are being used proportionately.

In his recent report, the IRTL suggested that current safeguards are deterring councils from seeking access to communications data.[1] Although the existing

safeguards should be maintained, there is a need to ensure that they are implemented in an efficient way that does not deter appropriate use of communications data.

Central government should ensure that councils are able to apply for and be granted magistrates approval electronically, in line with the recent Spending Review commitment to fully digitise the court system. [2]

Central government should also consider the case for routing all such applications through a small number of magistrates courts with direct links to the National Anti-Fraud Network. By creating centres of expertise, this would ensure that this safeguard is applied consistently and robustly.

There are already a number of safeguards attached to councils' access to communications data, specifically the requirements that it is:

- authorised by a director, head of service or service manager (or someone who holds a higher position),
- managed through the National Anti-Fraud Network, and,
- approved by a magistrates court.

Given these checks, it is unlikely that the proposed offence of unlawfully obtaining communications data could be incurred without deliberate intent to deceive, an action which might already be covered by existing offences such as misconduct in public office. The new offences of knowingly or recklessly acquiring communications data need to be very clearly defined within the Bill to distinguish between a genuine mistake and deliberate action. Furthermore it must be clear what the legal responsibilities and consequences are for inappropriate acquisitions submitted by an applicant, undertaken by a Single Point of Contact (SPOC) and authorised by a Designated Senior Officer (DSO).

Although we do not believe the new offences are strictly necessary, we recognise the intention to provide public assurance about proper use of the powers through the creation of a specific offence. We are confident that there will not be a need to invoke the offences proposed at Clause 9 of the Bill, for unlawfully obtaining communications data, in relation to council officers.

A single Judicial Commission

The creation of a single body to oversee the use of investigatory powers will be beneficial in terms of ensuring a consistent approach to the interpretation of key issues in the legislation. The different bodies with oversight of this area have in the past occasionally reached different interpretations of issues relevant to local authorities (for example, the DSO role): a single, consistent view will be helpful.

1 Further information on the Report of the Interception of Communications Commissioner http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

2 Further information on the Spending Review, paragraph 2.147 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/479749/52229_Blue_Book_PU1865_Web_Accessible.pdf

Case studies showing how councils use communications data
Set out below are a small selection of case studies outlining how local authorities have used communications data to identify criminal activity, and bring prosecutions against the perpetrators of those targeting vulnerable and elderly people in particular.

Operation Violet
Operation Violet led to the jailing of five members of a family for conning elderly people out of hard earned savings. The gang preyed on at least 81 victims who came from Yorkshire, Derbyshire, Staffordshire, Nottinghamshire and as far south as Essex. Trading Standards were only able to identify the gang and connect them with their victims through access to communications data.

The court heard they conned or tried to defraud them of £175,645, according to the charge sheet. However, the prosecution accepted the real number of victims and the scale of their losses was incalculable. A confiscation hearing under the Proceeds of Crime Act involved a claim of nearly £1 million.

Gang leader David Price Snr, 42, was given a sentence of seven years and eight months. His sons Abraham, 20, and David Jnr, 19, were sent to Young Offenders' Institutions for three years and eight months and three years and four months respectively. Angelina Price, 40, the leader's wife, was jailed for 16 months and his brother Shane, 41, was sentenced to three years and four months. Family associate James Cunningham, 26, from Castleford, West Yorkshire, was jailed for five years and four months.

Operation Crossbill
The initial subscriber check assisted in identifying the main perpetrator of a crime of fraud committed against an elderly vulnerable male. The subsequent itemised billing for the relevant period demonstrated calls were made to the victim from the perpetrators phone on the time and dates alleged by the victim and corroborates his story. The subscriber check requested thereafter was to confirm the telephone was being used by the money launderer. This demonstrated calls to the victim and calls to the perpetrator at the relevant times and thus again corroborated the victims story.

The telecoms data identified an offender and supported the allegation made by the victim. The total monetary value for this investigation was £8,100. Subsequent arrests and searches resulted in evidence of two further crimes.

Current case: Operation Travalger
Operation Travalger is a long-running fraud investigation into the activities of a number of suspects who defraud older consumers by means of cold calling, and then signing the victims up to roofing work which is unnecessary and involves the application of paint. False claims are made regarding the properties of this paint, and sums in the low thousands of pounds are generally extracted in return for the work. As the result of the particular subscriber check and itemised billing, a suspect was identified and two further individuals were arrested and are bailed until mid-January 2016 on suspicion of fraud. The data recovered from the further suspects' phones has yielded many more recent victims. It is anticipated that the suspects will be charged with fraud by false representation in January 2016.

It was solely as the result of the communications data that the further suspects and victims were identified. This tool is central and vital to the work that the regional investigation teams within Trading Standards do. It is used sparingly and proportionately; without access to this data it simply would not be possible to detect

the criminals the teams are dealing with.